EXHIBIT 256

**Exhibit
0012**
Cotton

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Kari Lake, *et al*,

 Plaintiffs,

 v.

Katie Hobbs, Arizona Secretary of State, *et al.*,

 Defendants.

)
)
)
)
)
)
)
)
)

No. 2:22-cv-00677-JJT

DECLARATION OF BENJAMIN R. COTTON

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an

oath. I make this affidavit of my own free will and based on first-hand information and

my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the

University of Maryland University College. I have numerous technical certifications,

including the Certified Information Systems Security Professional (CISSP), Microsoft

Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident

Response Examiner.

4) I have over twenty-six (26) years of experience performing computer forensics

and other digital systems analysis.

5) I have over nineteen (19) years of experience as an instructor of computer

1

forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6)   I have testified as an expert witness in state courts, federal courts and before the United States Congress.

7)   I have testified before the Arizona State Senate in public hearings on 15 July 2021 and 24 September 2021 concerning the digital forensics findings connected to the Arizona State Senate Maricopa County audit of the 2020 general elections. I fully stand behind those forensic findings. I have included my presentation to the State Senate, file name Senate Final Presentation.pdf, as Exhibit A to this affidavit.

8)   I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies and am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

9)   In the course of my duties I have forensically examined Dominion Democracy Suite voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, hereinafter referred to as the "Analyzed Elections Systems".

10)   In the course of my duties I have reviewed the administrative manuals and documentation for the Dominion Democracy Suite software and hardware components.

11)   In the course of my duties I have reviewed the public information from the Election Assistance Commission and its certification process for election software.

available, typically on a weekly basis. There is a systemic issue with all of the Analyzed Elections Systems. There was an antivirus program installed on each of the systems. None of the system's antivirus definitions had EVER been updated following the installation of the Dominion Democracy Suite Software. In terms of the Maricopa County election system, the antivirus software had not been updated for over 19 months. In practical terms, this means that the virus protection was so out of date that the system would not have prevented over five hundred seventy million (570,000,000) pieces of malicious code from compromising the voting system.

b) **Failure to Patch and Maintain Operating System (OS) Security** – The operating systems within the Analyzed Election Systems, including Windows, Linux and MacOS, contained vulnerabilities. These vulnerabilities could be exploited to gain unauthorized access to the targeted systems. Microsoft, the developer of the Windows software that was present on the Dominion PC-based Voting systems during my examination, releases operating system patches on a weekly basis to correct previously unknown operating system vulnerabilities and to prevent the possibility of unauthorized access to these systems. Based on my analysis of the Analyzed Election Systems in Maricopa County Arizona, Maricopa County Arizona, Fulton County Georgia, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, there is no evidence of a procedure or process to patch or fix the operating system vulnerabilities on the voting systems. None of these organizations had patched the operating systems

5

since the date that the Dominion Democracy Suite had been installed. In

Maricopa County, the Windows operating systems had not been patched for over

19 months and contained fixes (patches) for three thousand five hundred twelve

(3,512) known vulnerabilities directly applicable to the Maricopa County

Dominion voting system. A list of these vulnerabilities is included as a file

included with this report named, "Microsoft Patched Vulnerabilities between

August 2019 and April 2021.xlsx (md5 hash value:

D1E09A7C762E21653B1A28C3D9EE4E5E).

c) **Failure to Properly Establish and Control Assess to Voting Systems** - Based

on my review and consideration of the Analyzed Election Systems from different

jurisdictions it is apparent that there is a systemic problem with access controls to

the voting systems. In each case the usernames and passwords were established

concurrently with the installation of the voting software by the Dominion

employees. There are two major issues with the password management of these

systems. First, in all examinations of the Analyzed Election Systems, the

passwords were identical for all user accounts on that unique system. For each

unique jurisdiction, all passwords within that election system were the same for

all user accounts. Second, these passwords were never changed by the local

officials following the installation of the software. These two deficiencies result

in long-term shared password exposure for multiple elections. Furthermore,

there does not appear to be any accountability or assignment of the accounts to a

specific individual for specific time periods. This makes individual

6

20)   Based on my experience if the Cyber Security failures and lapses exhibited by the election systems networks and computers that I have examined were present in an enterprise that was subject to PCI or HIPAA industry certifications, that network would not be certifiable.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF JUNE 2022.
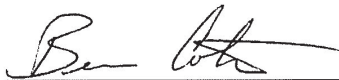
Benjamin R. Cotton

Exhibit A - Senate Final Presentation
Exhibit B - CyTech Taiwan Germany
Exhibit C - 2021.05.17 Response Letter to Senate President Fann -
                 FINAL_202105171430291332
Exhibit D - 033122 EAC Dominion Anomoly
Exhibit E - Antrim Lawsuit Exhibit 8 Benjamin Cotton Affidavit
Exhibit F - 081920 Halderman Declaration
Exhibit G - 080221 Halderman Decl.
Exhibit H - Special Master Final Report
Exhibit I - EMS Windows Log Files
Exhibit J - Microsoft Patched Vulnerabilities between August 2019 and April 2021

14